Information Security Attack Tree Modeling for Enhancing Student Learning

Jidé B. Odubiyi, Computer Science Department
Bowie State University, Bowie, MD
and
Casey W. O'Brien, Network Technology Department
Community College of Baltimore County, Baltimore, MD

WECS7, Naval Postgraduate School
Monterey, CA, January 4-6, 2006

Presentation Outline

- Introduction
- Background
- Instructional Approach
- Threat Modelling Process
- Lessons Learned
- Future Work
- Questions

Introduction: Course Offerings

Bowie State University

- Established in 1865. Current enrollment: 5K+ students
- CS Department: Offers BS and MS degrees in CS and Computer Technology
  - About 500 undergraduates and 40 graduate students
  - ABET Accredited
- Course Offerings:
  - Foundations of Computer & Network Security
  - Principles & Methods of IDS and IPS
  - Software & Operating System Security
  - Fundamentals of Cryptography and Applications
  - Cyber Law

Introduction: Course Offerings

Community College of Baltimore County (CCBC)

- Established in 1957. Current enrollment: 70,000 students
- Offers A.A. and A.A.S. degrees in Computer Science, Network Technology, and Information Systems
  - Middle States Commission on Higher Education Accreditation
- Course Offerings:
  - Introduction to Information Security (Security+)
  - Operating Systems Security
  - Network Defense and Countermeasures

Background

- Failure Mode and Effect Analysis (FMEA)
- Software error seeding and scenario analysis
- Threat modeling—Microsoft Tool
- The courses and student population
  - Fundamentals of Computer and Network Security (Spring 2005, 6 graduate students and 5 undergraduates)
  - Principles of Intrusion Detection and Prevention (Fall 2005, 2 undergraduates 8 graduate students)

Instructional Approach

- **Instructional Environment**

  - Lecture and Lab. Exercises using VMWare (USMA VIAN experiments with exploits)
  - Laboratory exercises modeling attack trees of the top 20 SANS vulnerabilities
  - Typical business enterprise—Network Operations Map (TOM)

Attack Tree Modeling and Attack Scenarios

SANS Institute Top-20 Vulnerabilities: Awareness

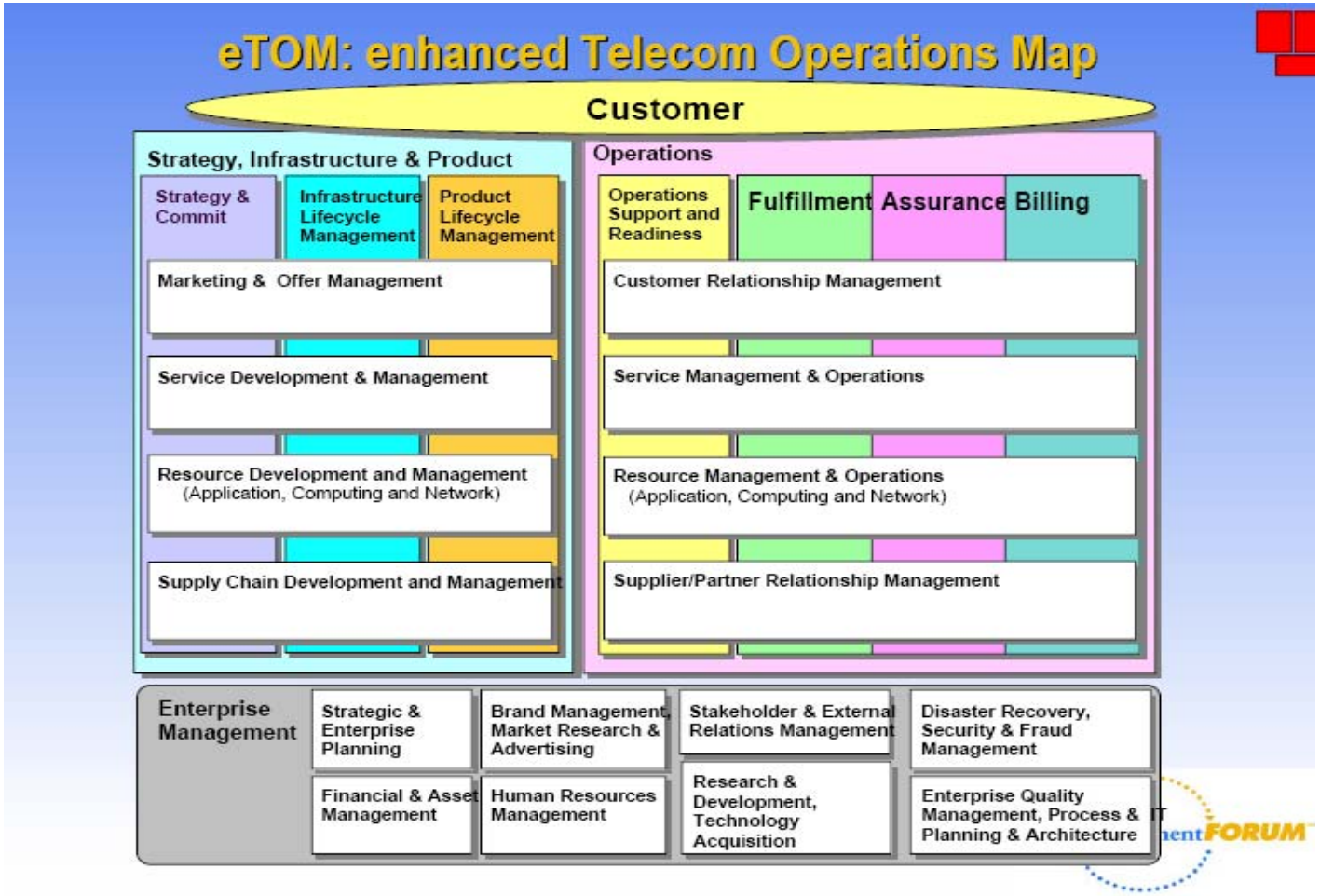
http://www.sans.org/top20/

- Top Vulnerabilities in Cross-Platform Applications
  - **C1. Backup Software**
  - **C2. Anti-virus Software**
  - **C3. PHP-based Applications**
  - **C4. Database Software**
  - **C5. File Sharing Applications**
  - **C6. DNS Software**
  - **C7. Media Players**
  - **C8. Instant Messaging Applications**
  - **C9. Mozilla and Firefox Browsers**
  - **C10. Other Cross-platform Applications**

Attack Tree Modeling and Attack Scenarios (cont'd)

- Top Vulnerabilities in Windows Systems
  - **W1. Windows Services**
  - **W2. Internet Explorer**
  - **W3. Windows Libraries**
  - **W4. Microsoft Office and Outlook Express**
  - **W5. Windows Configuration Weaknesses**
- Top Vulnerabilities in UNIX Systems
  - **U1. UNIX Configuration Weaknesses**
  - **U2. Mac OS X**
- Top Vulnerabilities in Networking Products
  - **N1. Cisco IOS and non-IOS Products**
  - **N2. Juniper, CheckPoint and Symantec Products**
  - **N3. Cisco Devices Configuration Weaknesses**

A Typical (Telecom) Business Enterprise



CCBC
The Community College of Baltimore County

WECS7, Naval Postgraduate School
Monterey, CA, January 4-6, 2006

BOWIE STATE UNIVERSITY
FLAME OF FAITH
TORCH OF TRUTH
MARYLAND
1865

Threat Modeling: Textual Description

GOAL: (G0) **Gain Privileged Access to a Web Server Using a Known Vulnerability**

AND G1. Identify organization's domain name.

G2. Identify organization's firewall IP address

OR 1. Interrogate domain name server

2. Scan for firewall identification

3. Trace route through firewall to Web server

G3. Determine organization's firewall access control

OR 1. Search for specific default listening ports

2. Scan ports broadly for any listening port

G4. Identify organization's Web server operating system and type

OR 1. Scan OS services' banners for OS identification

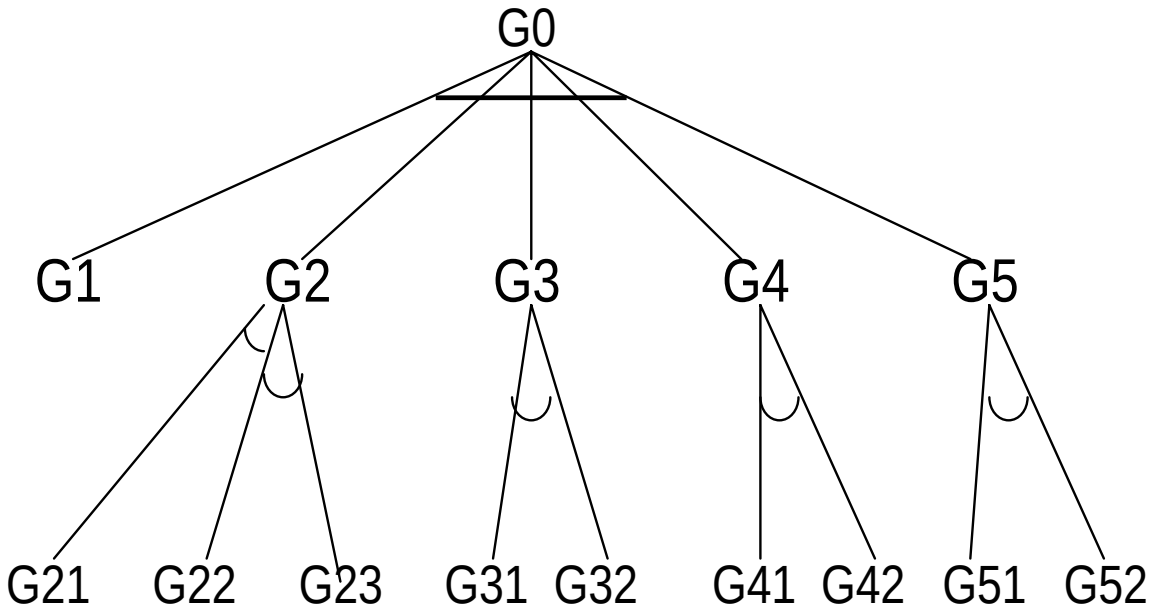
2. Probe TCP/IP stack for OS characteristic information

G5. Exploit organization's Web server vulnerabilities

OR 1. Access sensitive shared intranet resources directly

2. Access sensitive data from privileged account on Web server

Threat Modeling - Web Server Attack Graphical Representation



$$(G0 \equiv G1 \cap G2 \cap G3 \cap G4 \cap G5); (G2 \equiv G21 \parallel G22 \parallel G23)$$

Threat Modeling: 24 Attack Scenarios

[G1, G21, G31, G41, G51], [G1, G21, G32, G41, G51],
[G1, G21, G31, G42, G51], [G1, G21, G32, G42, G51],
[G1, G22, G31, G41, G51], [G1, G22, G32, G41, G51],
[G1, G22, G31, G42, G51], [G1, G22, G32, G42, G51],
[G1, G23, G31, G41, G51], [G1, G23, G32, G41, G51],
[G1, G23, G31, G42, G51], [G1, G23, G32, G42, G51]
[G1, G21, G31, G41, G52], [G1, G21, G32, G41, G52],
[G1, G21, G31, G42, G52], [G1, G21, G32, G42, G52],
[G1, G22, G31, G41, G52], [G1, G22, G32, G41, G52],
[G1, G22, G31, G42, G52], [G1, G22, G32, G42, G52],
[G1, G23, G31, G41, G52], [G1, G23, G32, G41, G52],
[G1, G23, G31, G42, G52], [G1, G23, G32, G42, G52]

Lessons Learned and Challenges

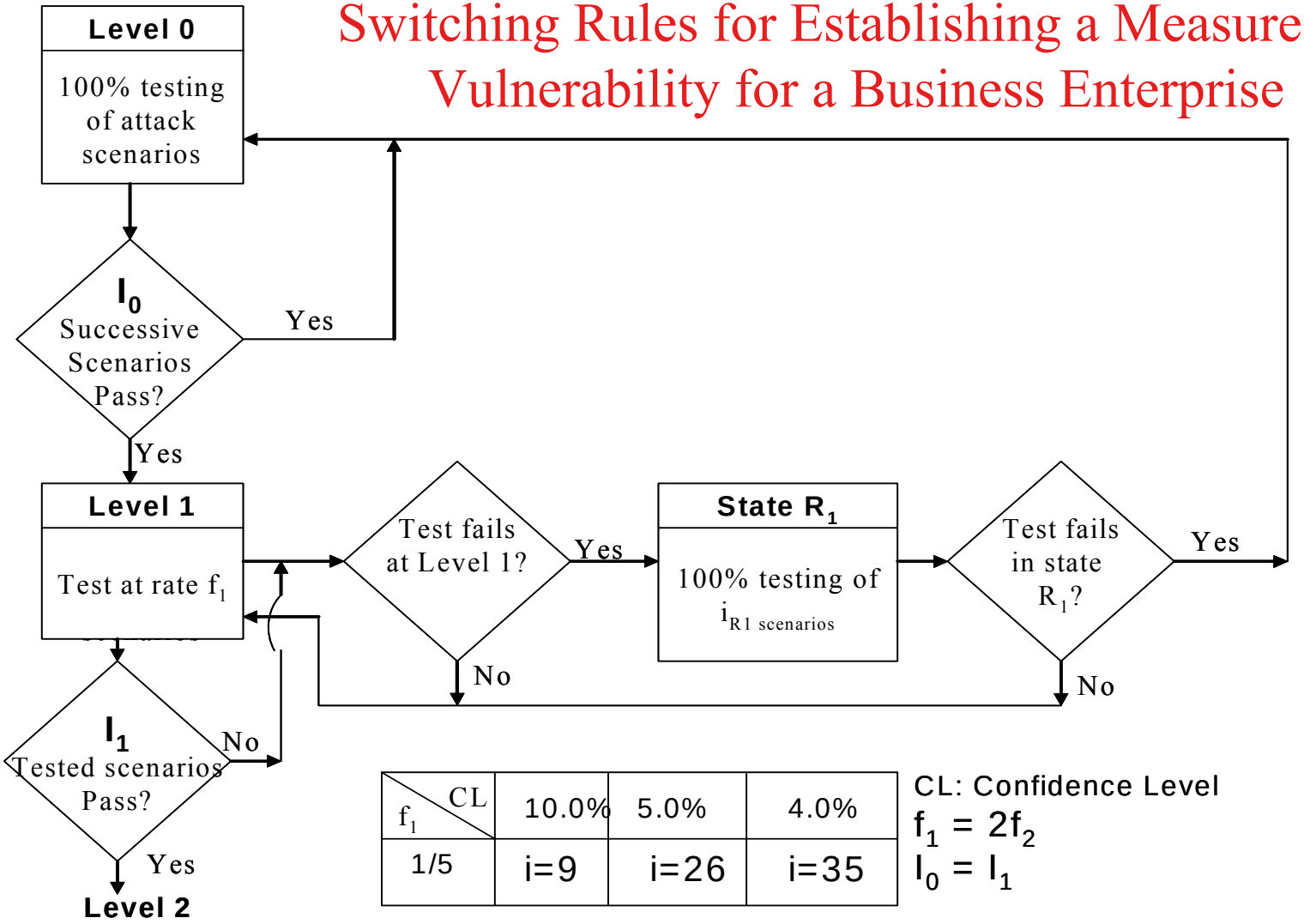
- Students' inability to think like hackers in modeling attack scenarios
  - Given a vulnerability, they tend to think in terms of what the system administrator should do rather than system exploitation strategies
- The challenge of modeling all possible attack scenarios--Coverage
- The challenge of testing the scenarios with some degree of confidence

Future Work

- Developing a system capability metric to support system vulnerability scanning and penetration testing

- Implement an algorithm for a system capability metric/framework for system administrators and Red teams

A Single Level Continuous Sampling Scheme with Switching Rules for Establishing a Measure of Vulnerability for a Business Enterprise



f_1 \ CL	10.0%	5.0%	4.0%
1/5	i=9	i=26	i=35

CL: Confidence Level

$f_1 = 2f_2$

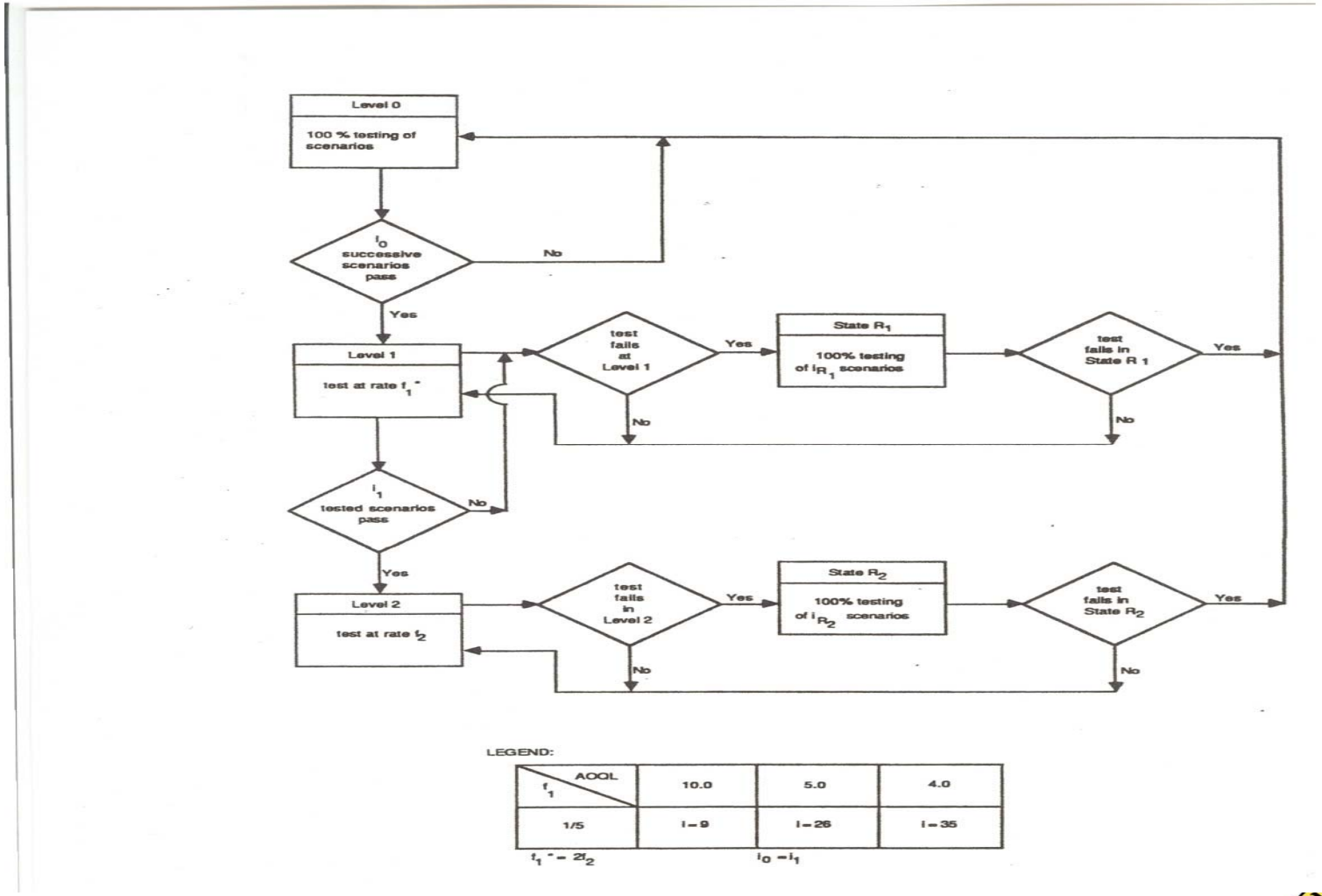
$I_0 = I_1$

CCBC
The Community College of Baltimore County

WECS7, Naval Postgraduate School
Monterey, CA, January 4-6, 2006

BOWIE STATE UNIVERSITY
FLAME OF FAITH
TORCH OF TRUTH
MARYLAND
1865

Future Work – Sampling Scheme



LEGEND:

f_1 \ AOOL	10.0	5.0	4.0
1/5	i – 9	i – 26	i – 35

$f_1^* = 2f_2$ $\quad i_0 - i_1$

CCBC
The Community College of Baltimore County

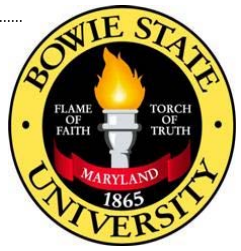
WECS7, Naval Postgraduate School
Monterey, CA, January 4-6, 2006

BOWIE STATE UNIVERSITY
FLAME OF FAITH · TORCH OF TRUTH
MARYLAND 1865

Questions?

Thanks for listening!

CCBC
The Community College
of Baltimore County



From An Attack Tree to An Attack Forest

Vulnerability Scanning versus Penetration Testing

Vulnerability scanning aims to identify potential problems based on known vulnerabilities

Penetration testing attempts to breach security defenses of a system by exploiting system vulnerabilities using hacking tools, etc.